

UNITED STATES DISTRICT COURT

for the
District of South Dakota

In the Matter of the Search of

Black in color Chevrolet Cruze, South Dakota license plate number Y4007, VIN 1G1PC5SBOF7200886, in the custody of the FBI, and a cellular phone contained within vehicle.

Case No. 5:19-mj-155

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the District of South Dakota (identify the person or describe the property to be searched and give its location):

Black in color Chevrolet Cruze, South Dakota license plate number Y4007, VIN 1G1PC5SBOF7200886, in the custody of the FBI, and a cellular phone contained within vehicle.

I find that the affidavit, or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal (identify the person or describe the property to be seized):

Evidence of a crime in violation of 21 U.S.C. § 841, as described in **ATTACHMENT A**, attached hereto and incorporated by reference,

I find that the affidavit, or any recorded testimony, establishes probable cause to search and seize the person or property.

YOU ARE COMMANDED to execute this warrant on or before January 3, 2020 (not to exceed 14 days)

☒ in the daytime 6:00 a.m. to 10 p.m. ☐ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Daneta Wollmann.
(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (check the appropriate box)

☐ for _____ days (not to exceed 30). ☐ until, the facts justifying, the later specific date of _____.

☐ I find that good cause has been established to authorize the officer executing this warrant to not provide notice prior to the execution of the search warrant, i.e., "no knock".

Date and time issued: 12-20-19 12:15pm


Judge's signature

City and state: Rapid City, SD

Daneta Wollmann, U.S. Magistrate
Printed name and title

cc: AUSA Nelson
ees

Return

Case No.:

5:19-MJ-155

Date and time warrant executed:

Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

*Executing officer's signature*_____
Printed name and title

UNITED STATES DISTRICT COURT

for the
District of South Dakota
Western Division

In the Matter of the Search of:

Black in color Chevrolet Cruze, South Dakota license
plate number Y4007, VIN 1G1PC5SBOF7200886, in
the custody of the FBI, and a cellular phone contained
within vehicle.

Case No. 5:19-mj-155

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

Black in color Chevrolet Cruze, South Dakota license plate number Y4007, VIN 1G1PC5SBOF7200886, in the custody of the FBI, and a cellular phone contained within vehicle.

located in the District of South Dakota, there is now concealed *(identify the person or describe the property to be seized)*:

See **ATTACHMENT A**, which is attached to and incorporated in this Application and Affidavit

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section
21 U.S.C. §§ 841

Offense Description

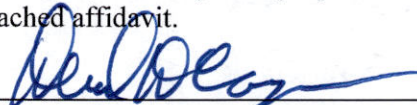
Possession with Intent to Distribute a Controlled Substance

The application is based on these facts:

☒ Continued on the attached affidavit, which is incorporated by reference.

☐ Your applicant requests that no notice be given prior to the execution of the search warrant, i.e., "no knock", the basis of which is set forth in the attached affidavit.

☐ Your applicant requests authorization to serve the search warrant any time day or night pursuant to Fed. R. Crim. P. 41(e)(2)(A)(ii), the basis of which is set forth in the attached affidavit.



Applicant's signature

Daniel Cooper, Special Agent, FBI

Printed name and title

Sworn to before me and: ☒ signed in my presence.

☐ submitted, attested to, and acknowledged by reliable electronic means.

Date: 12-20-19



Judge's signature

City and state: Rapid City, SD

Daneta Wollmann, U.S. Magistrate

Printed name and title

1. I am a Special Agent with the FBI, in Rapid City, South Dakota. I have been with the FBI since November 1991. I attended and successfully completed the FBI Academy in 1991. I have been stationed in Rapid City for approximately 18 years. I am assigned to investigate primarily drug offenses as they relate to communities on the Pine Ridge Reservation. I am a member of the Badlands Safe Trails Drug Task Force.
2. The following information is based on investigation by fellow Federal Bureau of Investigation special agents, the United States Marshals Service, Oglala Sioux Tribe Department of Public Safety officers, and the South Dakota

Highway Patrol. This affidavit does not contain the entirety of my knowledge regarding this investigation.

ITEMS TO BE SEARCHED:

3. This affidavit is made in support of an application for a search warrant to search for and seize evidence of a violation of Title 21 U.S.C. § 841, which the possession with intent to distribute a controlled substance. The items that are the subject of the search and seizure applied for in this affidavit are specifically, a black in color Chevrolet Cruze, South Dakota license plate number Y4007, VIN 1G1PC5SBOF7200886, and a cellular phone contained within the vehicle.
4. I submit there is probable cause to search for evidence, fruits, and instrumentalities of the following violations of criminal law: 21 U.S.C. § 841.
5. The applied-for warrant would authorize the search and seizure of items contained with the vehicle identified above, complete processing of the vehicle, and the forensic examination of the cellular phone within the vehicle for the purpose of identifying electronically stored data.

Modus Operandi of Drug Traffickers

6. During my tenure in law enforcement, I have been involved in numerous investigations of narcotic trafficking organizations involving the distribution of controlled substances and the amassing and concealing of the proceeds of these sales. I have interviewed drug users and dealers regarding the manner in which they operate and have become familiar with their techniques. I have executed search warrants for vehicles, residence, hotel

rooms, as well as search warrants for devices, records, ledgers, and documentation reflecting the sale of controlled substances.

7. Based upon my training and experience, including my direct experience in this investigation, I have developed knowledge regarding practices commonly used by drug traffickers and their organizations, including:

- A. Drug traffickers often maintain, on hand, large amounts of cash (typically U.S. currency) in order to finance their drug distribution activities;
- B. It is common for drug traffickers to secrete contraband (including controlled substances), proceeds of drug sales, and records of drug transactions in secure locations within their residences, business, in lock boxes/safes and vehicles to conceal them from law enforcement.
- C. Drug traffickers commonly maintain addresses or telephone numbers in books, documents and electronic devices that have memory which include computer hard drives, cellular phones, Global Positioning Systems which reflect names, addresses and telephone numbers of the associates in the trafficking organization.
- D. I also know that individuals involved in the distribution of controlled substances and their associates correspond and communicate using internet, social media, email, cellular phone text messages and that their computers and/or other electronic storage media in their possession may be used to prepare, create, and maintain writings, records, and documents relating to their activities and associations, including but not limited to the trafficking of controlled substances.
- E. Through my own experience and training, I am aware that it is common for narcotics traffickers to utilize cellular telephones to facilitate their drug trafficking activities. I am also aware that in addition to using the telephones for communication purposes, said traffickers may also use the internal memory (such as "phone book" or "notes" functions) of the telephone to store names, identifying information, and contact telephone numbers of individuals involved in said drug-trafficking enterprises, and that certain models of cellular telephone also maintain limited logs of past calls made by that telephone.
- F. I am also aware that more people, including drug traffickers, are utilizing "Smart" phones, such as Apple iPhones, and GPS units for travel directions. These GPS units can be standalone devices manufactured for that single purpose or applications used through cellular phones. Many of the "Smart" phones and GPS units are programmed with addresses from around the United States and all a user has to do is enter the address he/she wants to travel to and the "Smart" phones and GPS units will provide a travel route for the user. Besides providing a travel route for the user most of the "Smart phones" and GPS units also automatically

keep track of the route the user has taken and will back track the route to the point of origin.

- G. Drug traffickers take or cause to be taken photographs and videos of themselves, their associates, their assets, their travels, and their product. That these traffickers usually maintain these photographs and videos in their possession, or within their residences, computers, cellular phones, vehicles, and/or other locations over which they maintain dominion and control;
- H. It is generally a common practice for drug traffickers to maintain in their residences and/or other locations over which they maintain dominion and control records relating to their drug trafficking activities. Because drug traffickers in many instances will "front" (that is, sell on consignment) controlled substances to their clients, or alternatively, will be "fronted" controlled substances from their suppliers, such record-keeping is necessary to keep track of amounts paid and owed, and such records will also be maintained close at hand so as to readily ascertain current balances. Often drug traffickers keep "pay and owe" records (drug ledgers) to show balances due for drugs sold in the past ("pay"), and for payments expected ("owe") as to the trafficker's supplier and the trafficker's dealer(s). Additionally, drug traffickers must maintain telephone and address listings of clients and suppliers, and keep them immediately available in order to efficiently conduct their drug trafficking business. Such records can be maintained on paper, cellular phones, or other devices.
- I. It is a generally common practice for drug traffickers to make use of wire transfers, cashier's checks, and money orders to pay for expenses associated with services to facilitate their illegal activities. Evidence of such financial transactions and records relating to income and expenditures of money and wealth in connection with drug trafficking would also typically be maintained in a trafficker's residence and/or other locations over which they maintain dominion and control, including cellular phones.
- J. I am also aware that a Subscriber Identity Module ("SIM") card is a portable memory chip predominantly used in cellular phones that hold information regarding the cell phone's number, address, book, text messages, and other data. SIM cards can typically be removed from a phone and placed in another phone, retaining its original data. SIM cards usually have a unique number associated with it so that it can be associated with a particular cell phone service provider.
- K. Drug dealers keep paraphernalia for packaging, weighing, using and distributing controlled substances and the paraphernalia include, but are not limited to, scales, plastic bags, aluminum foil, paper bindles, zip lock bags and other containers commonly used to package and store controlled substances.
- L. Drug distributors frequently trade illegal drugs for stolen property and firearms.

M. Drug distributors frequently possess firearms in the furtherance of their drug activities, such as intimidation or threats.

DEFINITIONS

8. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. *Computer*: The term "computer" means "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device." See 18 U.S.C. §§ 2256(6) and 1030(e)(1). As used herein, a computer includes a cell phone, smart phone, tablet, and other similar devices capable of accessing the Internet.
- b. *Computer Hardware*: The term "computer hardware" means all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices such as video gaming systems, electronic music playing devices, and mobile phones); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, modems, routers, scanners and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).
- c. *Computer Passwords and Data Security Devices*: The term "computer passwords and data security devices" means information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates a sort of digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.
- d. *Computer Software*: The term "computer software" means digital information which can be interpreted by a computer and any of its

related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

- e. *Computer-Related Documentation:* The term "computer-related documentation" means written, recorded, printed, or electronically stored material which explains or illustrates how to configure or use computer hardware, computer software, or other related items.
- f. *Internet:* The "Internet" is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.
- g. *Internet Connection:* The term "Internet connection" means a connection required for access to the Internet. The connection would generally be provided by cable, DSL (Digital Subscriber Line), wireless devices, or satellite systems.
- h. *Storage Medium:* The term "storage medium" refers to any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.
- i. *Visual Depictions:* "Visual depictions" include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. See 18 U.S.C. § 2256(5).
- j. *Wireless Network:* The term "wireless network" means a system of wireless communications in which signals are sent and received via electromagnetic waves such as radio waves. Each person wanting to connect to a wireless network needs a computer which has a wireless network card that operates on the same frequency. Many wired networks base the security of the network on physical access control, trusting all the users on the local network. But, if wireless access points are connected to the network, anyone in proximity to the network can connect to it. A wireless access point is equipment that connects to the modem and broadcasts a signal. It is possible for an unknown user who has a computer with a wireless access card to access an unencrypted wireless network. Once connected to that network, the user can access any resources available on that network to include other computers or shared Internet connections.

SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

9. Based upon my training and experience and information related to me by agents and others involved in the forensic examination of computers, I know that computer data can be stored on a variety of systems and storage devices

including hard disk drives, floppy disks, compact disks, magnetic tapes and memory chips. I also know that a search of computer equipment and storage devices must be taken to a laboratory or facility that has specialized knowledge and training in the extraction of data from the equipment for the following reasons:

- a. Searching computer systems is a highly technical process which requires specific expertise and specialized equipment. There are so many types of computer hardware and software in use today that it is impossible to bring to the search site all of the technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may also be necessary to consult with computer personnel who have specific expertise in the type of computer, software application or operating system that is being searched;
- b. Searching computer systems requires the use of precise, scientific procedures which are designed to maintain the integrity of the evidence and to recover "hidden," erased, compressed, encrypted or password-protected data. Computer hardware and storage devices may contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Since computer data is particularly vulnerable to inadvertent or intentional modification or destruction, a controlled environment, such as a law enforcement laboratory, is essential to conducting a complete and accurate analysis of the equipment and storage devices from which the data will be extracted;
- c. The volume of data stored on many computer systems and storage devices will typically be so large that it will be highly impractical to search for data during the execution of the physical search of the premises; and
- d. Computer users can attempt to conceal data within computer equipment and storage devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension ".jpg" often are image files; however, a user can easily change the extension to ".txt" to conceal the image and make it appear that the file contains text. Computer users can also attempt to conceal data by using encryption, which means that a password or device, such as a "dongle" or "keycard," is necessary to decrypt the data into readable form. In addition, computer users can conceal data within another seemingly unrelated and innocuous file in a process called "steganography." For example, by using steganography a computer user can conceal text in an image file which cannot be viewed when the image file is opened. Therefore, a substantial amount of time is necessary to extract and

sort through data that is concealed or encrypted to determine whether it is evidence, contraband or instrumentalities of a crime.

10. Based on my own experience and my consultation with other agents who have been involved in computer searches, searching computerized information for evidence or instrumentalities of a crime often requires the seizure of all of a computer system's input and output peripheral devices, related software, documentation, and data security devices (including passwords) so that a qualified computer expert can accurately retrieve the system's data in a laboratory or other controlled environment. There are several reasons that compel this conclusion:

- a. The peripheral devices that allow users to enter or retrieve data from the storage devices vary widely in their compatibility with other hardware and software. Many system storage devices require particular input/output devices in order to read the data on the system. It is important that the analyst be able to properly re-configure the system as it now operates in order to accurately retrieve the evidence listed above. In addition, the analyst needs the relevant system software (operating systems, interfaces, and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media), as well as all related instruction manuals or other documentation and data security devices; and
- b. In order to fully retrieve data from a computer system, the analyst also needs all magnetic storage devices, as well as the central processing unit (CPU). In cases like the instant one where the evidence consists partly of image files, the monitor and printer are also essential to show the nature and quality of the graphic images which the system could produce. Further, the analyst again needs all the system software (operating systems or interfaces, and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media) for proper data retrieval.

PROBABLE CAUSE

11. On December 19, 2019, the Oglala Sioux Tribe Department of Public Safety (OST DPS) received a dispatch call regarding a suspicious vehicle.

The vehicle was identified and later confirmed to be a black in color Chevrolet Cruze, South Dakota license plate number Y4007, VIN 1G1PC5SBOF7200886.

12. On December 19, 2019, an officer with the OST DPS located the vehicle and conducted a traffic stop. The driver and only occupant, later identified as Uriah Lafferty, provided a false name to the officer. As the officer was dealing with the traffic stop, Lafferty fled the scene and a pursuit was initiated.
13. The pursuit continued off the Pine Ridge Indian Reservation toward Scenic, South Dakota, and ultimately into Custer County, South Dakota. During the course of the pursuit, a deputy with the United States Marshals Service assisted, as well as a second officer with OST DPS, and a South Dakota Highway Patrol officer.
14. After the pursuit continued for some time, Lafferty turned down a dead end and law enforcement was able to partially barricade Lafferty's vehicle using law enforcement vehicles.
15. After partially barricading Lafferty, law enforcement attempted to get Lafferty to get out of his vehicle. Lafferty was not compliant with commands and ultimately law enforcement ended up breaking the driver's window in an attempt to detain Lafferty. Law enforcement deployed both a taser and OC spray, but Lafferty continued to resist the officers and was not compliant.
16. Lafferty was able to put his vehicle in reverse and accelerated away from the officers who were attempting to physically detain him. Lafferty

then began to travel in the direction of the perimeter officers positioned behind the vehicle. As Lafferty accelerated toward them, the deputy United States Marshal fired multiple rounds into the vehicle at Lafferty. Lafferty was still able to drive forward and then fled.

17. After Lafferty fled, the pursuit continued until Lafferty's vehicle went off the road and got stuck in a ditch. Officers again attempted to detain Lafferty, who continued to be non-compliant and refused to produce his concealed right hand. Eventually officers were able to arrest Lafferty by physically removing him from his vehicle. Lafferty suffered a gunshot wound to his right arm.

18. After officers had Lafferty detained, they conducted a search of Lafferty. Officers located a bag containing approximately ½ ounce of a substance that field tested positive for methamphetamine and a black digital scale. Your affiant knows from training and experience that a digital scale is indicative of distribution. Your affiant knows from training and experience that ½ ounce of methamphetamine is not generally considered user amount but is an indication of distribution of controlled substances.

19. Officers then, without going into the vehicle, observed, from a position of plain view, four possible bullet holes in the vehicle, blood, drug paraphernalia, and could hear a cell phone alerting/ringing.

20. The vehicle was towed and is currently being stored at the FBI.

CONCLUSION

Based on the foregoing, your affiant respectfully requests a search warrant be

issued for a black in color Chevrolet Cruze, South Dakota license plate number Y4007, VIN 1G1PC5SBOF7200886, currently in the custody of the Federal Bureau of Investigation (FBI), and to permit law enforcement to completely search and process the vehicle, including the cellular phone contained within the vehicle.

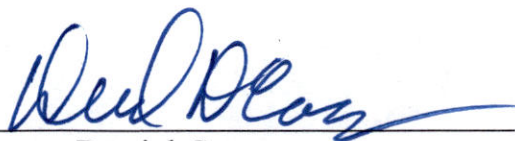
REQUEST FOR SEALING OF APPLICATION/AFFIDAVIT

21. I request that the Court order that all papers submitted in support of this application, including this affidavit, the application, the warrant, and the Order itself, be sealed for a period of 180 days. These documents discuss an ongoing criminal investigation that is neither public nor known to all the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may give targets an opportunity to flee, destroy or tamper with evidence, change patterns of behavior, notify confederates, or otherwise seriously jeopardize the investigation.

Further your affiant saith not.

Dated: _____

12-20-19



Daniel Cooper
Special Agent, Federal Bureau of
Investigation

SUBSCRIBED and SWORN to before me
this 20th day of December, 2019.



DANETA WOLLMANN
U.S. MAGISTRATE JUDGE

ATTACHMENT A

DESCRIPTION OF ITEMS TO BE SEIZED

The evidence, fruits, and or instrumentalities of violations of 21 U.S.C. § 841

1. All controlled substances.
2. Books, records, receipts, notes, ledgers, photographs and other papers relating to the importation, transportation, ordering, purchase and distribution of controlled substances.
3. All items determined to have been used or likely to be used for the packaging, weighing, transportation, shipping, use, distribution, storage, or processing of any controlled substance, including safes.
4. Vessels, implements and furniture used in connection with the manufacture, production, storage or dispensing of such drugs together with articles of personal property tending to establish the identity of the person(s) in control of contraband related paraphernalia.
5. All U.S. or foreign currency, or other forms of monetary instruments, or other financial commodities including precious metals, or other negotiable instruments, including re-fillable debit cards and receipts indicating the sending or possession of such cards.
6. Papers, tickets, notes, schedules, receipts, and other items relating to domestic and international travel.
7. Indications of occupancy, residency, and/or ownership of the premises described herein, including but not limited to utility and telephone bills, envelopes, rent receipts, repair bills, credit cards receipts, keys and articles of clothing.
8. Vehicle titles, registrations and other paperwork tending to show the identification of ownership and/or controlling parties of vehicles.
9. All contact lists, ledgers, calendars, notes, spreadsheets, diaries, contact information and appointment books to identify conspirators, customers, enforcers, or suppliers potentially involved in violating 21 U.S.C. §§ 841(a)(1) and 846.
10. Books, records, receipts, bank statements and records, money drafts, letters of credit, money orders, cashier's checks, receipts, passbooks, bank checks, safe deposit box keys, storage locker keys, and other items of evidencing the obtaining, secreting, transfer, and/or concealment of assets and the obtaining, secreting, transfer, concealment and/or expenditure of money.

This is meant to include any record reflecting the rental of a storage locker, rental facility, or other property, including hotel rooms, in which controlled substances could be stored.

11. Firearms, ammunition, paraphernalia associated with the possession and/or use of firearms, including but not limited to holsters, cases, or receipts indicating the purchase or sale of such items.
12. Call history information on the landline phone for the residence, to include the playing and recording of any messages left on any telephone answering device located on the premises.
13. Surveillance devices, cameras, etc.
14. Cell phones, tablets, and computers capable of being used to facilitate or document the distribution, sales, trafficking, or possession of controlled substances, along with any and all information contained on these devices to include, but not limited to:
 - a. Text messages;
 - b. Telephone lists and call logs;
 - c. All contact information, names, aliases, and telephone numbers stored in the phone, including any telephone number directory stored in the memory of the phone;
 - d. The content of any and all voicemail messages;
 - e. Browser history, including, but not limited to, "bookmarked" or favorite web sites and search terms entered into internet search engines;
 - f. Email messages;
 - g. Deleted data, receipts, notes, ledgers, and other information relating to the possession, sale and transfer of controlled substances;
 - h. All images, photographs and videos;
 - i. Any and all records, showing dominion, ownership, custody, or control over the phone.
15. Blood swabs taken from the interior and exterior of the vehicle.
16. Fingerprints taken from the interior and exterior of the vehicle.